Mobile Future: Pathways to Continued Improvement in Mobile Security and Privacy

Discussion Paper

May, 2021

CENTER FOR CYBERSECURITY
POLICY AND LAW

About the Center

The Center for Cybersecurity Policy and Law is a nonprofit (503(c)(6)) organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of those in the industry including members of civil society and government entities in the area of cybersecurity and related technology policy. The Center seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies and standards that will encourage professionals, companies, and groups of all sizes to take steps to improve their cybersecurity practices.

More information about the Center, its initiatives, and how you can get involved can be found at https://centerforcybersecuritypolicy.org.

Executive Summary

Over the past decade, consumers and businesses have turned to mobile devices and their applications (apps) for productivity, social networking, entertainment, e-commerce, and more. Apps are now commonly used to share personal information on social media, get directions, check prescriptions and bank balances, order dinner, make in-person and online retail payments, and even attend work or school. However, both the public and private sectors are increasingly innovating and expanding their investments in apps into far more consequential areas, such as healthcare. Therefore, a secure and privacy-respecting mobile ecosystem is more than simply desirable, it is essential, and the models and approaches to achieving security and privacy controls within that ecosystem must not be compromised in a way that increases risk to end users.

As cybersecurity experts across the digital economy struggle to keep pace with ever-evolving threats, advancements in mobile security and privacy offer a vision into how security can be done properly while enabling continuous improvement. While new threats to mobile devices continue to arise, the protections in place are generally working better than in other areas of cybersecurity. It is imperative to understand why this is, how it came to be, and to ensure that policymakers do not make decisions that could weaken these protections.

The Center for Cybersecurity Policy and Law ("Center") established this project to help further the discussion around this important subject. This paper draws on research of previously published information on the topic, and multi-stakeholder focus groups hosted by the Center to discuss the risks, approaches, and desired outcomes for enabling the security and privacy of mobile apps and the app stores that support them.

The focus groups represented a wide range of viewpoints and sectors including commercial, academic, civil society, and current and former government, and included international views. With such a diverse and outspoken group, topics and debates were considerable, but ultimately, there was consensus support for the following assertions:

- **The state of security and privacy on mobile platforms has continued to improve over time, although that improvement has not been even across different ecosystems.**
- **Building security and privacy into platforms and apps from the start is the most effective way to reduce risk to users**.
- **Most users cannot be expected to defend themselves effectively**.
- **Policies that address mobile ecosystems must not weaken the security of those ecosystems**.

While these assertions do not represent the entirety of the discussion, they are the key points that bring together the general sense of the participants in the context of security and privacy. Topics outside that context were not in scope for the discussion. The Center would like to thank all the participants for their time, commitment, and expertise.

Discussion

The state of security and privacy on mobile platforms has continued to improve over time, although that improvement has not been even across different ecosystems.

Right from the start, members of the focus group noted that years ago, when mobile devices began becoming truly prevalent in our business and personal lives, they did not envision that secure mobile ecosystems would be truly possible; and that those ecosystems have manifested and are now often more trusted than most other networked devices, is in part a response to how they have become nearly ubiquitous across all aspects of modern life.

Growth and Adoption

Since the first mobile phones took root in the marketplace decades ago, mobile phone ownership has experienced sustained growth alongside continuous technological evolution. What started as a 'dumb' device affordable to a relative few and whose primary purpose was to provide its user audio communication free from geographic constraints, has since developed into a 'smart' internet connected, multifunctional necessity used by billions across the globe. Indeed, mobile devices have become one of the most sophisticated consumer devices ever built, and that sophistication continues to grow.

Recent estimates have suggested that there are more than 5.50bn unique mobile subscribers globally, up from just over 4.00bn at the start of 2015.[1] This includes the estimated 3.78bn individuals, nearly half the world's population, that were classified as mobile internet users by the end of 2019, an increase of roughly 250m from the previous year.[2] These mobile phone and mobile internet users are increasingly made up of smartphone device users. The uptake in smartphone devices, while comprising a higher total in more traditionally developed international regions, has seen tremendous

[1] https://www.ericsson.com/4adc87/assets/local/mobility-report/documents/2020/november-2020-ericsson-mobility-report.pdf

[2] https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf

growth in all regions over just the past few years.[3] Globally, the estimated share of smartphones as a percentage of mobile connections has risen from just over 30% in 2014, to just under 70% by 2019.[4]

The growing adoption rates of mobile devices alongside their improving technological capabilities has subsequently expanded the activities that they are used for. No longer just a means of audio communication, mobile devices are used to access news and government services, manage personal banking and finance, pay for utilities and services, and are even used to look for employment opportunities.[5] In mobile banking and finance for example, Business Insider reported in 2021 that 89% of respondents to their *Mobile Banking Competitive Edge Study* affirmed they use mobile banking, and in 2018, Bloomberg reported that there were 396 million registered mobile-money accounts within sub-Saharan Africa alone.[6][7]

In the healthcare and public health sector, mobile devices have become nearly essential to the dissemination of timely information, for tracking illnesses, and for ensuring communication among providers and their patients. Increasing trends in telehealth have relied heavily on apps and mobile devices to reach remote populations and to provide healthcare during the global pandemic.

This trend of growing activities tied to mobile devices is supported by the massive influx of mobile apps being downloaded from prominent app stores. Current estimates suggest there are over 2.2m apps on Apple's App Store and 3.3m apps on Google's Play Store.[8] Furthermore, estimates from market intelligence firms suggest that mobile application downloads have risen significantly over the past few years. One such firm reports that mobile application downloads from just Apple's iOS App Store and Google's Play Store jumped from 15.8bn in Q1 of 2015 to 33.6bn in Q1 2020.[9]

While Apple's App Store and Google's Play Store are clearly the main places to find apps, there is certainly no shortage of third-party sources for mobile device users to engage with. A 2020 study on key trends in mobile enterprise security conducted by Wandera estimated that there are over 300 app stores worldwide and that number continues to grow.[10] This is important because it is estimated that a significant number of Android and iOS device users engage with third-party app stores as well as sideloading. For example, Wandera's research notes that one in five Android users have their

[3] https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf

[4] https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf

[5] https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf

[6] https://www.businessinsider.com/mobile-banking-market-trends

[7] https://www.bloomberg.com/news/articles/2019-08-13/mobile-phones-are-replacing-bank-accounts-in-africa

[8] https://www.businessofapps.com/guide/app-stores-list/

[9] https://www.businessofapps.com/data/app-statistics/

[10] https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/wanderas-web-gateway-for-mobile/mobile-threat-landscape-2020-whitepapers.pdf

devices configured to allow third-party app installations and that iOS device users that had at least one sideloaded app jumped from 3.4% in 2018 to 5.8% in 2019.[11]

Most app stores, regardless of mobile platform or owner, have a similar functionality and aesthetic that end users have come to recognize and expect. Searching for the app you want and installing it to your device is practically seamless even though the apps themselves can come from developers of widely varying skill, goals, and business drive. Despite these similarities, app stores themselves are far from equal. The risk to end users can increase dramatically with the uncertain motivations or security and privacy controls in place around a third-party app store. In fact, Crowdstrike notes that "The majority of mobile malware is distributed from third-party sources that do not perform comprehensive checks of applications they provide."[12]

Just how that checking is done can vary widely:

- A fully curated approach with significant control and review exercised by the app store owner that often combines automated tools with human analysis to identify security and privacy risks;
- A partially curated approach with limited control and review exercised by the app store owner that may still use automated tools but has limited-to-no human review;
- An un-curated approach with no controls or review process exercised by the app store owner; or
- Sideloading without an app store.

When considered in the context of end user security and privacy, these models are not equal in the protections they can provide.

Of these, sideloading is arguably the riskiest to uninformed end users, although that risk is offset somewhat by the fact that side loading often requires a level of technical expertise that many end users simply don't possess. In simple terms, sideloading involves installing an app onto a mobile device outside the context of an app store, such as downloading the app package from a web site and installing it directly. How easy that is accomplished depends a great deal on the mobile platform. For example, while it is possible to sideload apps on Apple iOS, it is not easy for an average consumer, and, this process is not officially supported. Android OS on the other hand, allows sideloading, if the user has explicitly enabled the function as it is disabled by default.

Similarly, a completely un-curated app store is akin to making sideloading easier for multiple apps. As with direct sideloading, end users still must enable the app store to be accessible on their device, and once that is done, any app on that store can be loaded.

[11] https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/wanderas-web-gateway-for-mobile/mobile-threat-landscape-2020-whitepapers.pdf

[12] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

On the other end of the spectrum is the fully curated app store where the owner constructs an ecosystem that tightly integrates the hardware, operating systems, apps, and even payment systems. While this model certainly doesn't mean that no unwanted, malicious, or fraudulent apps will find their way onto a user's device, it does dramatically reduce the likelihood of that happening. The most commonly cited company that takes this type of approach is Apple. CrowdStrike's *2019 Mobile threat Landscape* Report noted that "While the Apple mobile ecosystem is not immune to malicious software, there are barriers to development and deployment of potentially malicious software the complicates the typical deployment techniques … often used to install Android-based RATs[remote access trojans]."[13]

This makes it clear that how an app store owner chooses to interact with their users has a direct impact on their user's risk, and that the underlying complexities involved in making informed security decisions is beyond the knowledge of most users.

Most users cannot be expected to defend themselves effectively.

Users are conditioned to trust that their software, hardware, and service providers are taking all the security steps to protect them, and they have little to no responsibility themselves. Even while that may not always be true, there are elements to security that the average end user would never be able to reasonably understand and address effectively.

Mobile platforms are susceptible to many types of malware and both non-state criminal actors and nation-state actors waste little time in developing new malware or adapting existing malware to the mobile environment. CrowdStrike's *2019 Mobile threat Landscape Report* found that "the targeting of mobile platforms is increasingly being adopted by a range of criminal and targeted intrusion adversaries," and that "development capability has proliferated to less-skilled groups due to the accessibility of proof-of-concept mobile malware variants."[14] According to the same report, the most prevalent types of mobile malware encountered are remote access tools (RATs), stalkerware, banking trojans, ransomware, cryptojacking, and adware.[15]

The growing attention that the mobile environment has garnered from malicious actors is also reflected in a rapid increase of detected malware and potentially unwanted applications (PUA).[16] On Android OS for example, research institute AV-TEST noted a significant increase in the amount of detected malware and PUA beginning in 2014.[17] According to additional statistics compiled by AV-TEST, the total average amount of malware and PUA detected on Android OS between 2012 and

[13] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

[14] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

[15] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

[16] PUA are "applications installed in a mobile device … that may pose high risk or have untoward impact on user security and/or privacy." *Trend Micro*

[17] https://portal.av-atlas.org/malware/statistics

2013 was just over 2 million, whereas between 2015 and 2019 the total average was roughly 7.8 million.[18]

Similar challenges exist with regards to digital privacy which has garnered considerable attention in recent years as more end users have come to understand how much data is collected about them and how it gets used. Factoring in the types of data, such as medical and financial, that mobile apps are processing and storing, the concern becomes that much greater. While some suggest that most users simply don't care as long as their app works the way they want and the data is not stolen by malicious actors, others would say that users should at least have the ability to make informed decisions about whether they are okay with how the app will treat their data. Traditionally, this has been handled via often long and complex privacy policies, but according to a 2019 Pew Research survey "…only about 20% of Americans overall say they always (9%) or often (13%) read these policies before agreeing to them, and 36% say they never read them."[19] That strongly suggests that simply making information available to users is not the same as educating them in a meaningful way.

Given the extent and complexity of the risk, expecting end users to have the requisite understanding of security and privacy and how to protect themselves via layered on security, esoteric, or hard-to-find settings, and other methods simply isn't viable at scale. To do so would make users the last line of defense against far more sophisticated bad actors taking advantage of not only complexity, but the inherent trust users place in the devices. Further, if practices such as sideloading were to become easier and more commonplace, it would be that much more difficult for users to differentiate between what is "good" and what is "bad", further increasing the risk.

RESEARCHERS

Both focus groups noted the importance of the security researcher community in identifying vulnerabilities in mobile platforms and app stores. It was suggested that more open mobile ecosystems have benefited considerably from allowing greater access for researchers, and in fact Google has had a robust program for engaging with researchers for many years. More recently, Apple has been working to engage with researchers more effectively both through a bug bounty program, as well as providing a version of the iPhone designed specifically for researchers.

The focus groups felt strongly that security and privacy are enhanced when developers, service providers, and researchers can build and maintain trusted relationships, and would like to see these efforts

This is why most reputable app stores have made significant efforts to build ecosystems that work hard to reduce the risk to users long before an app is ever downloaded to a mobile device.

[18] https://portal.av-atlas.org/malware/statistics

[19] https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

Building security and privacy into platforms and apps from the start is the most effective way to reduce risk to users.

While there may still be considerable onus placed on end users to secure their technology and data via security mechanisms that are implemented on top of or around apps and services, there has been a steady shift toward building better security and privacy into products and services from the start, so that end users have less to worry about.

This can be achieved in several different ways including:

- Developing code that meets security best practices and implementing appropriate security and privacy controls.
- Using automated tools to scan for vulnerabilities, weaknesses, and other potential issues.
- Using human reviewers to evaluate app functionality.

For the apps themselves, incentivizing and enabling app developers to write software and deploy services that meet adequate security controls is a critical first step. There are many sources of information and guidance on how to write secure code including from the National Institute of Standards and Technology (NIST),[20] BSA | The Software Alliance,[21] and SafeCode,[22] among others.

The existence of this guidance makes it clear that writing secure code is possible and there are certainly many developers that do so. Increasing awareness and implementing market drivers to encourage others is worth consideration but incentives do not always motivate developers and publishers to take those steps if they remain confident that their apps will sell regardless.

For app store owners, advances in automated scanning tools has led to a marked reduction in the number of malicious apps on their stores.

According to RiskIQ's 2020 Mobile App Threat Landscape report, overall blacklisted apps (apps that appear on at least one official blacklist, such as VirusTotal) dropped a total of 67% from 2019.[23] Google's Play Store showed an impressive 59.9% reduction in blacklisted apps since 2019, their second annual reduction.[24] The use of automated scanning tools has played a significant role in achieving these results.

Where these tools are less useful is uncovering potentially fraudulent behavior that isn't related to software vulnerabilities, specifically but may attempt to get users to enter sensitive information without fully disclosing for what purpose. Fraud can also include attempts by apps to collect

[20] https://csrc.nist.gov/Projects/ssdf

[21] https://www.bsa.org/files/reports/bsa_software_security_framework_web_final.pdf

[22] https://safecode.org/

[23] https://www.riskiq.com/resources/research/2020-mobile-threat-landscape-report/

[24] https://www.riskiq.com/resources/research/2020-mobile-threat-landscape-report/

payment information without clearly disclosing that it is required prior to the app being installed. In these cases, human reviews can be a good mechanism for identifying these apps and having them removed from the app store. Apple's App Store has been effective using this approach, so much so that AV-TEST does not even track threats on iOS because there are simply so few. That is not to say that those threats don't exist. Instances of malware do arise[25] and scam apps continue to be a problem, despite the review processes in place.[26]

Additionally, the way that mobile devices are configured by default and what options are available can directly impact user security and privacy. As noted previously, the easier it is for users to sideload apps, either intentionally or accidentally, the more likely the entire ecosystem suffers in the aggregate through the spread of malware, fraudulent apps, and so forth.

The point is that when app store owners and developers take security and privacy enhancing actions, users benefit in ways they likely aren't aware of, and that require nothing of them. Also, it's worth noting that none of this precludes users from choosing from an ever-increasing multitude of apps available within an app store to meet their needs. The goal of enhancing security and privacy at the app and app store level should not be to reduce the number of available and competing apps, but to reduce the number of apps that can proved to be harmful.

Of course, all of this depends on the app store owner being motivated to engage in security and privacy enhancing activities which certainly isn't always the case, and the risk this creates for users hasn't gone unnoticed by policymakers.

Policies that address mobile ecosystems must not weaken the security of those ecosystems.

As the technology around mobile devices and apps continues to grow and evolve, policymakers around the world are looking to come to terms with its impacts and what role government has in overseeing and managing the technology, as well as the massive amounts of data involved.

Many of the high-profile cases to date have been centered around issues with data privacy, such as with Cambridge Analytica,[27] where among other things, the use of data on individuals was used in ways the individuals never intended to consent to. This led to numerous hearings in both the United States and the United Kingdom and has since led to various fines and calls for legislative changes. There have also been significant privacy impacting policies in the past few years including the California Consumer Protection Act (CCPA) and the General Data Protection Rule (GDPR), and there will very likely be more. While these laws and policies have largely been seen by experts to enhance privacy and security, the focus groups expressed the need to remain diligent in ensuring that future

[25] https://threatpost.com/click-fraud-malware-apple-app-store/149496/

[26] https://9to5mac.com/2021/04/07/scam-ios-apps-latest-a-vpn-that-charges-9-99-week-uses-recommended-by-apple-pop-ups/

[27] https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

privacy rules could harm security and security rules could harm privacy. This serves as a tacit acknowledgement that, while privacy and security are mostly connected today, it is a delicate balance to continually improve on both. Striking that balance requires that security experts, privacy advocates, and technology companies work with policymakers to educate them while also listening to and understanding the challenges they are attempting to address on behalf on their constituents.

One place where this dynamic is already playing out involves competition related policies that could require operating system vendors to allow sideloading or otherwise allow app makers to skip the automated and human review processes that have become essential to providing the security and privacy that users expect.

Simply put, in an effort to protect or empower their constituents, well-intentioned policymakers could end up causing harm in unintended, but potentially serious ways. Doing so could unravel years of dedicated hard work by major mobile platform companies and app store owners who have made the security of their customers a priority. This is not to say that policymakers should not hold companies that don't take security and privacy seriously accountable. Modern society's dependence on mobile devices, and the fact that they are under constant threat, compels them to do so.

Conclusion

Security and privacy-respecting capabilities in the technology on which society depends is an essential part of our personal and professional lives and mobile ecosystems are a major part of that. Without the right protections in place, our mobile devices, and the information they hold become easy targets for criminals, fraudsters, political adversaries, and others.

The wide-ranging experts brought together by the Center arrived at four primary assertions:

- **The state of security and privacy on mobile platforms has continued to improve over time, although that improvement has not been even across different ecosystems.**

- **Building security and privacy into platforms and apps from the start is the most effective way to reduce risk to users**.

- **Most users cannot be expected to defend themselves effectively**.

- **Policies that address mobile ecosystems must not weaken the security of those ecosystems**.

Taken together, these assertions suggest that those who can have the most direct impact on the mobile ecosystem (i.e. app developers and app store owners) bear a significant responsibility for protecting their users and have generally taken that responsibility seriously. Correspondingly, the threat and risk has also increased and will continue to do so as use and reliance on mobile devices and services grows. Managing that risk will require innovation, rigor, and commitment, that must not be hindered by policies that do not prioritize security and privacy.

Appendix A: Focus Groups

In March 2021, the Center invited recognized security and privacy experts to share their views in an open discussion designed to capture both the current state of affairs with mobile security, and with an eye towards the future. While both events were held under Chatham House Rules, the individuals below agreed to have their names listed here, with the understanding that inclusion in this list is no way an endorsement of the assertions or recommendations made by the Center.

Focus Group Attendees

Jaya Baloo, Avast
John Banghart, Center for Cybersecurity Policy and Law
Alissa Cooper, Cisco
Sam Curry, Cybereason
Michael Daniel, Cyber Threat Alliance
Joseph Lorenzo Hall, Internet Society
David Hoffman, Intel
Jane Horvath, Apple
Kent Landfield, McAfee
Maggie MacAlpine, Cybereason
Jonathan Mayer, Princeton
Michael Ogata, NIST
Jeff Ratner, Apple
Michelle Richardson, Center for Democracy and Technology
Jim Routh, Retired
Ross Schulman, New America
Ari Schwartz, Center for Cybersecurity Policy and Law
Murugiah Souppaya, NIST
Amie Stepanovich, Silicon Valley Flatirons, University of Colorado School of Law
Megan Stifel, Global Cyber Alliance
Vanja Svajcer, Cisco
Stephen Unger, Flint Global
Beau Woods, I am the Calvary

The Center would like to thank each of these individuals for their contributions to this important topic, both during the focus group sessions and through their daily efforts.